SECTIGO®

2020 WORK-FROM-HOME IT IMPACT STUDY

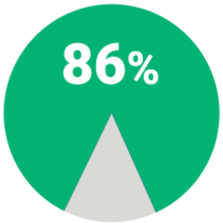
WAKEFIELD

WAKEFIELDRESEARCH.COM

Executive Summary

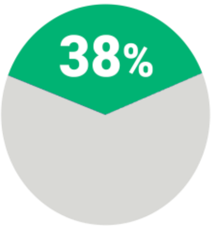
The sudden arrival of COVID-19 ushered in a new IT paradigm as workers worldwide transitioned from offices to work-from-home (WFH) environments full-time. **A survey of 500 IT professionals at companies of at least 1,000 employees in the U.S., Canada, Germany, France, Ireland and the UK., revealed that the transition to widespread remote work presented myriad business challenges and security risks for the employees on the front lines of IT security.** This survey was conducted across industries and includes additional insights on IT professionals in U.S. banking to capture challenges in their field. While many IT professionals saw an increase in employee productivity at their company, they also saw new and dangerous risks emerge—and despite the clear and present danger, many companies remain at-risk as proven long-term IT security strategies have not been fully implemented.

The transition to widespread remote work revealed myriad challenges faced by those workers on the front lines of IT security:



In all, 86% of IT professionals report challenges in managing the digital identity of users, devices, and processes at their companies. In the U.S. banking industry, the rise of risk is even more dire: 93% report challenges to managing digital identity of users, devices, and processes at their companies.

Nearly half (49%) of IT professionals feel employee productivity at their company has increased since the start of widespread remote work, while another 35% feel it's stayed consistent. Only 16% say productivity decreased.



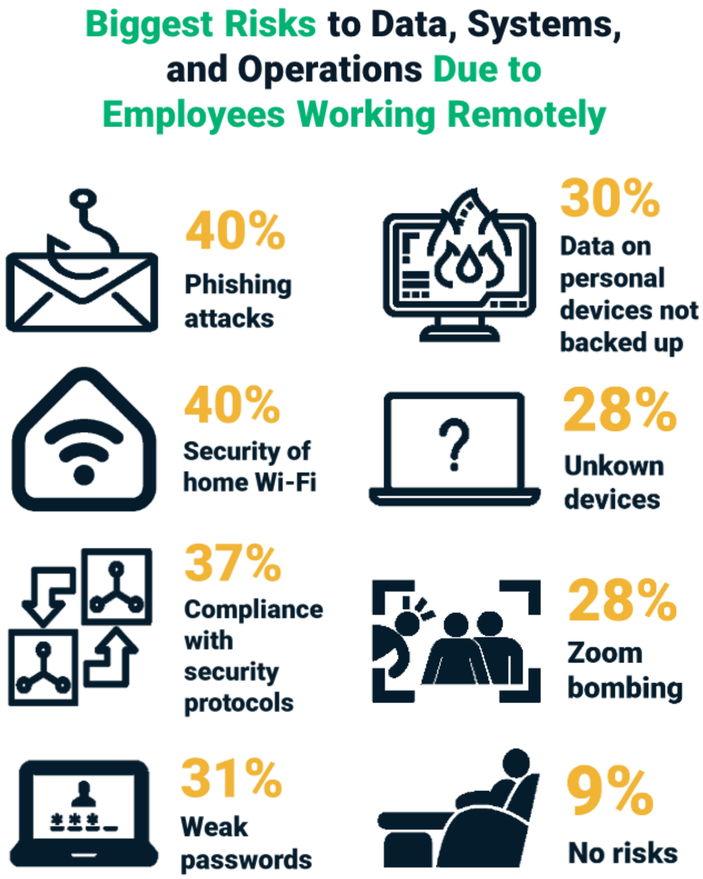
As they adjusted to this new work model, companies bottom lines were affected: **38% of IT professionals say their company delayed revenue-generating initiatives for 4+ weeks as a result of adjusting to widespread remote work.**

Despite risks, nearly 3 in 5 IT professionals (59%) expect the number of remote workers to increase after offices reopen. This includes 17% who expect it to increase *significantly*. IT professionals working in U.S. banking are even more optimistic: 72% expect an increase in remote work.

Identity Management Risks in WFH Models

IT professionals are already spending their days putting out fires and doing everything they can to keep their data secure. But the switch to remote work took an already fraught security environment and exacerbated it.

With the vast majority of IT professionals (86%) reporting challenges in managing digital identity of users, devices, and processes at their companies, certain challenges rise to the top: **the biggest challenge is data management complexities, which 45% of IT professionals face, followed closely by rapid changes to digital identity/authentication solutions (44%).** The third-most-common challenge is managing secure access across BYOD devices (36%).



Biggest Risks to Data, Systems, and Operations Due to Employees Working Remotely

40% Phishing attacks

30% Data on personal devices not backed up

40% Security of home Wi-Fi

28% Unkown devices

37% Compliance with security protocols

28% Zoom bombing

31% Weak passwords

9% No risks

In the financial world, security is paramount yet IT professionals in U.S. banking face even more challenges to managing digital identity—and interestingly, their most common challenges differ from their global peers. **IT professionals in U.S. banking are most likely to cite managing access across BYOD devices (64%) as the greatest risk**, followed by rapid changes in digital identity/authentication solutions (62%), data management complexities (52%), and lack of skilled cybersecurity professionals (50%).

And challenges are more common at smaller companies with fewer resources. **Companies with fewer than 10,000 employees (89%) are more likely than companies with 10,000 or more employees (76%) to report facing challenges.**

The rise of widespread remote work compounds IT professionals' concerns, with new risks emerging as a result of employees working at home. **Nearly all (91%) report risks of having employees working remotely without in-person oversight.** Notable risks include phishing (40%), security of home or remote Wi-Fi (40%), and compliance with company-mandated security protocols (37%). Again, this is even more pronounced among U.S. banking IT professionals, with an overwhelming 98% reporting risks of having employees working remotely as well, especially compliance with company-mandated security protocols (48%), phishing (47%), Zoom bombing (42%), and data on personal devices not being backed up (40%).

The rise in remote work points to an increased effort by IT professionals to manage all the risks of data access management, even as they already had to address a wide array of challenges.

BYOD

Using personal devices can be an easy fix for a remote work model, which could be why **60% of IT professionals report employees using personal devices during widespread remote work**, especially at companies with fewer than 10,000 employees (64%, compared to 44% of companies with 10,000 or more). These personal devices include laptops (41%) smart devices (31%), and desktop computers (30%). While BYOD might be convenient, the practice can also make IT professionals' jobs more difficult as they address making an employee's device secure: **36% of IT professionals say management of access across BYOD is a challenge to managing digital identity of users, devices, and processes at their company.**

Personal devices are a less-common problem in U.S. banking, where only 39% of IT professionals say employees are using personal devices. **Nevertheless, 64% of IT professionals in U.S. banking say managing access across BYOD devices is one of the biggest challenges they face in managing digital identity, the most commonly cited challenge among these professionals.**

Opening the Floodgates to Remote Work—Despite Hazards

While many IT professionals were not prepared for the sudden adoption of widespread remote work, they nevertheless predict that their companies are going to increase their remote workers even after their offices reopen. But in doing so, they need to carefully consider how adjusting to widespread remote work caught them off guard—and do everything they can to ensure that they are more prepared.

Nearly two-thirds of IT professionals (65%) report that their company did not have extensive remote work infrastructure set up prior to the COVID-19 outbreak. Instead, 33% quickly invested in systems to enable remote work and 31% either bootstrapped existing systems or made no changes at all. IT professionals in U.S. banking report these similar numbers, with 65% who also did not have extensive remote work infrastructure set up, showing that they were similarly caught off guard.

2 in 5 IT professionals report taking more than a week to set up remote work systems.

Quick assemblies were more common at smaller companies, where 34% bootstrapped a remote work setup or made no changes, significantly more than the 22% of companies with 10,000+ employees who either bootstrapped or made no changes to their remote work setup.

But while companies might have been able to adjust to their new remote work setup, they did not necessarily do so quickly. **Two-fifths of IT professionals (41%) report that their company took more than a week to completely set up their business' remote work systems—in fact, 11% said it took them more than a *month*.** Even more IT professionals in U.S. banking (45%) say it took more than a week.

Beyond this initial period of setup, ensuring the success of remote work even put revenue initiatives and cybersecurity initiatives on the backburner: **38% of IT professionals say their company delayed revenue-generating initiatives for a month or more.** Nearly as many IT professionals in U.S. banking (35%) report a delay in revenue-generating initiatives lasting a month or longer.

Alongside having to delay revenue initiatives, IT professionals also had to delay improvements to how they manage the risks they were scrambling to avoid: **44% say they delayed cybersecurity initiatives for a month or longer. Such lengthy delays were even more common among U.S. banking IT professionals, with more than half (56%) reporting delays of at least one month in order to prioritize the success of remote work.** Both of these delays came in order to prioritize the success of remote work.

Nearly 2 in 5 delayed revenue-generating initiatives for a month or longer.

But even now, as most IT professionals believe they are facing increased risk—risk that comes on top of preexisting challenges, as well as the difficulties of remote work setup that delay other important initiatives—not all companies have made great strides to incorporate the right data security at their companies. **A surprising 73% of IT professionals report they have not significantly increased their company's data security as a result of remote work setup—including 30% who saw no increase whatsoever.** Over half of U.S. banking IT professionals (52%) report that they have also not significantly increased cybersecurity. How will IT professionals address these increased risks without proper investment, especially when a lack of preparation was responsible for delayed initiatives to begin with?

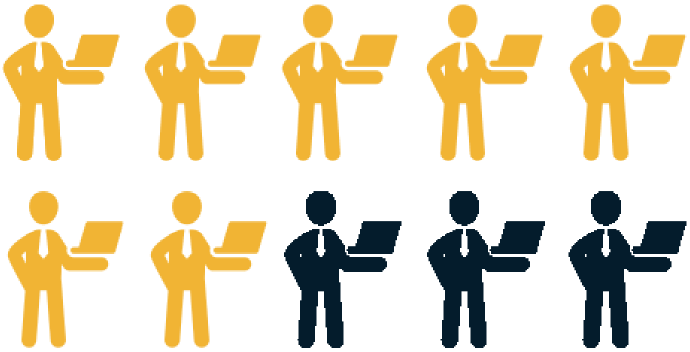
Authentication and Compliance

If IT professionals aren't doing enough, the consequences could be dire in the moment their data is breached and their protocols are investigated. But many IT departments have relatively few security protocols in place. More than 2 in 5 (44%) report that their companies are using only one or two security measures to protect their networks, applications, and other systems from unauthorized access.

Companies are using a mix of security measures to authorize access. Many use strong and proven authentication technologies, including identity certificates (56%) and biometrics (26%), in some capacity. **However, IT professionals are also using several methods with known weaknesses, including traditional username and password (65%) and hardware-token multi-factor authentication (50%).**

But while IT professionals are using this array of security protocols, they remain uncertain that their digital identity management meets the standards that they could be held to in the event of an audit or investigation. **A startling 71% of IT professionals don't feel completely confident that their company can report full compliance with industry and government standards on digital identity during remote work.**

This lack of confidence could be stemming from how much IT professionals anticipate increases in data security. **Those who don't expect to increase data security measures after offices reopen are more likely (77%) to report that they do not feel completely confident, significantly more than those who do expect increased data security (66%).**



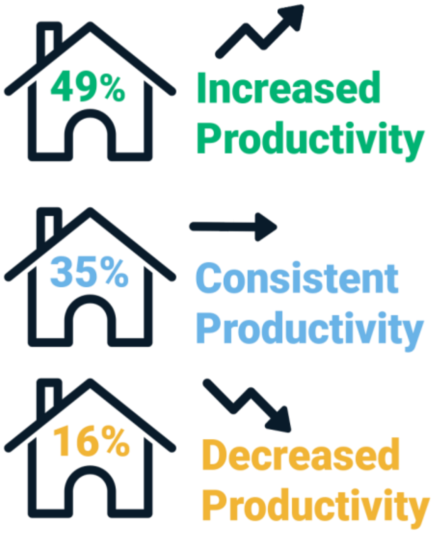
71% don't feel completely confident that they are in full compliance with industry and government standards for digital identity during remote work.

Banks are held to particularly rigorous standards, but nevertheless 56% of IT professionals in the U.S. banking industry are not completely confident their company is fully complying with industry and government standards related digital identity during remote work.

When More Productivity Means More Risk

One reason IT professionals predict an increase of remote work post-COVID could be that widespread remote work during the outbreak had a surprising effect: an increase in productivity. **In fact, nearly half of IT professionals (49%) saw an increase in employee productivity at their company during widespread remote work, and 35% feel it remained consistent even after the initial setup.** Increased productivity is especially common at companies with fewer than 10,000 employees (52%, compared to 39% at bigger companies). Those who saw this increase in productivity are predicting increased remote work accordingly: those who feel productivity has increased (73%) are justifiably more likely than those who say productivity has not increased (46%) to feel remote work will increase.

Nearly half of IT professionals feel their work's productivity has increased since the begging of widespread remote work, another 35% feel it's stayed consistent, and just 16% feel it's decreased.



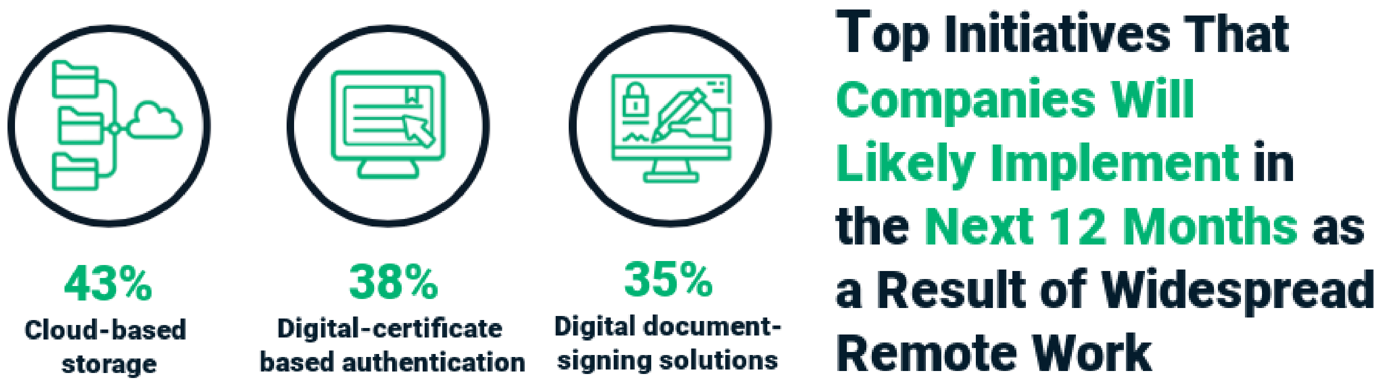
But while IT professionals recognize the benefits of remote work, they're less confident that post-COVID investment will meet their needs when it comes to mitigating risk. **While the majority of IT professionals acknowledge risks to their business with a remote workforce, 82% of IT professionals say that they do not expect their company to significantly increase security for their data and applications once offices reopen.**

IT professionals at companies that saw an increase in productivity, however, are more likely to say their companies are investing accordingly: **those who saw increases to productivity during remote work (70%) are more likely than those who did not see increased productivity (47%) to expect their company to increase data and application security after reopening offices.**

In this case, it seems that companies that experienced early benefits are willing to invest in initiatives to keep up their progress—but companies that did not see those benefits are leaving themselves open to risk. In fact, this is in keeping with a pattern of previous investment in security: **those who increased data security as a result of widespread remote work (68%) are more likely than those who did not increase data security (38%) to expect their company to increase data and application security after reopening offices.**

Security Initiatives

Whether or not investment will significantly increase, IT professionals nevertheless expect to be spending a lot of time on security initiatives next year: **93% expect that in the coming 12 months, their company will be more likely to act on an IT measure that improves security and business continuity due to widespread remote work.**



Cloud-based storage (43%) is the most likely to be increased, which makes sense given how remote work has shaken up conventional file access models. But alongside this obvious change, many IT professionals predict more security-minded initiatives. **Use of digital certificate-based authentication (38%) and use of digital document-signing solutions (35%) are also top initiatives that IT professionals see as more likely to increase in the coming 12 months.** Nearly as popular are mobile solutions, including increased use of mobile app-based authentication (34%), and access to systems and processes from mobile devices (33%).

Interestingly, 29% predict that their company is more likely to use biometric solutions in the next 12 months as the result of widespread remote work, whereas 28% predict more use of traditional username and password authentication, indicating expanded use of both new and traditional solutions with distinct levels of access security.

And increased authentication might be particularly necessary among the 26% who predict their company will be more likely to allow BYOD access to internal networks and data.

Even as IT professionals consider this array of initiatives, many are letting others pass under their radar. **Only 25% predict their company is more likely to use LaaS or PaaS as the result of widespread remote work, and even fewer predict more interest in use of desktop as a service (22%) or S/MIME-protected email (17%).**

Conclusion

The switch to remote work can involve sidelining cybersecurity measures, as well as postponing revenue-generating initiatives, possibly for weeks at a time. But if companies see the potential of increased productivity over the long term—and if the times are changing to a remote work model regardless—then they will need to be aware of the risks and, more importantly, how to mitigate them.

- Increased risks in remote work models put companies' data and systems in danger—and at the very least, companies face the added complications that come with not meeting industry or government standards during an outside investigation or audit.

- But the increase in productivity that many well-prepared companies saw during the rise of widespread remote work during the COVID-19 outbreak could mean that companies will move forward with widespread remote work despite these risks.

- As a result, it is increasingly essential not to shortchange investment in new security initiatives, or to continue using weak security measures. U**ser identity certificates offer advantages over phone- or token-based multi-factor authentication and simplify the process for remote employees to connect. With PKI-based certificates, employees' identity certificates are stored directly on their computer, laptop, or mobile phone, enabling authentication without any action—increasing an organization's overall security posture.** (Three Ways PKI Can Help Secure the Remote Workforce, a Sectigo White Paper, guides IT professionals through assessing and optimizing authentication technologies).

METHODOLOGICAL NOTES

The 2020 Work-From-Home IT Impact Study was conducted by Wakefield Research (www.wakefieldresearch.com) between May 15th and May 26th, 2020, among 500 IT professionals at companies of at least 1,000 employees, with 250 in the U.S. and Canada, 150 in Germany, France and Ireland, and 100 in the UK. The 2020 Work-From-Home IT Impact Study – U.S. Banking was conducted between May 15th and May 26th, 2020, among 100 US IT professionals working in banking or credit unions with at least 1,000 employees.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. For the interviews conducted in the Sectigo Survey, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 4.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample. For the interviews conducted in the Sectigo Survey – US Banking, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 9.8 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

ABOUT SECTIGO

Sectigo is a leading cybersecurity provider of digital identity solutions, including TLS/SSL certificates, DevOps, IoT, and enterprise-grade PKI management, as well as multi-layered web security. As the world's largest commercial Certificate Authority with more than 700,000 customers and over 20 years of experience in online trust, Sectigo partners with organizations of all sizes to deliver automated public and private PKI solutions for securing webservers, user access, connected devices, and applications. Recognized for its award-winning innovation and best-in-class global customer support, Sectigo has the proven performance needed to secure the digital landscape of today and tomorrow.

For more information, visit www.sectigo.com and follow @SectigoHQ.

ABOUT WAKEFIELD RESEARCH

Wakefield Research is a leading, independent provider of quantitative, qualitative, and hybrid market research and market intelligence. Wakefield Research supports the world’s most prominent brands and agencies, including 50 of the Fortune 100, in 70 countries. Our work is regularly featured in media.

To learn more, visit: www.wakefieldresearch.com

WAKEFIELD

WAKEFIELDRESEARCH.COM